CONTRADICTIONS IN THE LITERATURE OF GROUP THEORY.

By G. A. MILLER, University of Illinois.

PRESIDENTIAL ADDRESS DELIVERED BEFORE THE MATHEMATICAL ASSOCIATION OF AMERICA, SEPTEMBER 6, 1922.

The ancient Greeks, even before the time of Euclid, assumed that if two hypotheses lead to contradictory results they cannot both be true, and in Euclid's *Elements* frequent use is made of a method of proof known as *reductio ad absurdum,* called by the Greeks "reduction to the impossible." The "impossible" here often meant a result which contradicted a result which was assumed to be well established. While contradictions are so distasteful to the normal mind they have not been completely avoided in the mathematical literature. For instance, even Euclid used the term circle both for a curve and also for the area inclosed by this curve, and the double meaning of this particular term has persisted to our day. The seriousness of contradictions in the literature of our subject is illustrated by following well-known dictum due to Poincaré: "Mathematics is the art of giving the same name to different things." [1]

Many contradictions have been so mellowed by age that they are scarcely noticed by the teacher while the student is greatly perplexed by them. As teachers we cannot be too careful to point out emphatically where such contradictions appear. While this might seem to be a sufficient reason for the choice of the present subject for this extraordinary occasion, it may be admitted that the real reason was much more personal. A referee of a paper which I offered for publication did not agree with me in view of the fact that we used different definitions of the same term. Both of these definitions were sanctioned by long usage but it was only after considerable correspondence that the real source of the difficulty became clear. Hence I address you on this subject in somewhat the same state of mind as that exhibited by the rich man in the Bible who wanted Abraham to send Lazarus to testify to his five brethren "lest they also come into this place of torment."

The source of the particular difficulty to which I have just referred proved to be the fact that both in abstract group theory and in substitution group theory we commonly say that a given finite group is transformed into itself only by the operators or the substitutions of its holomorph. Hence some operators or substitutions transform such a group into itself while other operators or substitutions do not have this property. On the other hand, every possible operator or substitution transforms a given group into a simply isomorphic group, and all the simply isomorphic groups are usually regarded as the same group when abstract groups or regular substitution groups are listed. Hence we also say, at least implicitly, that a given group is transformed into itself by every possible group operator or by every possible substitution.

[1] *Bulletin des Sciences Mathématiques,* vol. 32, 1908, p. 174.

While the statements to which I have just referred seem to me to involve a contradiction, yet the facts involved in these statements are so well known that the student familiar with group theory is usually not apt to be disturbed thereby. Difficulties are more apt to arise in the newer developments where the contradictions to which we have just referred present themselves in a new form. For instance, a characteristic operator of a group is defined as an operator which must correspond to itself in every automorphism of the group. In particular, the identity is a characteristic operator of every possible group of finite order.

If all the simply isomorphic groups are regarded as the same, the identity is the only characteristic operator that can appear in a group, for every other operator can be transformed into an operator which is not itself by means of some group operator. Hence such an operator cannot be characteristic under the one of the two given definitions of the same group for this operator can be transformed into a different operator by means of an operator which transforms this group into a simply isomorphic group. In this simple isomorphism, or automorphism, the operator in question would therefore not correspond to itself.

It is evidently desirable to call some operators characteristic which are not the identity. In fact, this desirability is clearly reflected in a well-established custom. Moreover, it is not difficult to present the matter in such a way that no ambiguity arises as a result of this custom. It is only necessary to say that a characteristic operator is one which corresponds to itself in every possible automorphism arising under the holomorph of a group; if other automorphisms are regarded as possible, as is sometimes done, a characteristic operator does not necessarily correspond to itself in these automorphisms.

When I first studied this question it seemed to me best to say that a characteristic operator must correspond to itself in every possible automorphism in accord with the common definition. If this view is adopted it is necessary to say that if we establish a (1, 1) correspondence between the operators of two groups in such a way that a characteristic operator does not correspond to itself, the two groups cannot be regarded as the same group. This was done in an article by the present writer published in the *Proceedings of the National Academy,* volume 7, 1921, page 146.

It seems to me now wiser to modify the definition of characteristic operator as suggested above and to state explicitly that in group theory we employ two extreme definitions of what is meant by the same group. According to one of these definitions a characteristic operator must correspond to itself in every possible automorphism of the group while this is not the case when the other definition is under consideration. If this is done the corrections to which the article noted at the end of the preceding paragraph is devoted are uncalled for.

In addition to the two extreme definitions of the expression *the same group* there is a third which is still older but relates only to non-regular substitution groups of finite order. This was implicitly employed by A. L. Cauchy in his enumeration of the substitution groups whose degrees do not exceed 6 (*Comptes Rendus,* Paris, volume 21, 1845, pp. 1363 and 1401). A necessary and sufficient

condition that two substitution groups are the same, according to this definition, is that one of them can be transformed into the other by means of some substitution. The most general definition of what is meant by the same group can be obtained from this oldest definition by adding the condition that the two substitution groups in question shall be regular and therefore implies that a necessary and sufficient condition that two groups are the same is that a simple isomorphism can be established between their substitutions or operators. The other extreme definition implies that two groups are the same if and only if they involve the same substitutions or operators irrespective of the arrangement of these substitutions or operators within the group.

Just as the two different definitions of the term circle have persisted for at least two and a half millenniums, so these three different definitions of the expression *the same group* may reasonably be expected to persist. When new terms relating to these definitions are introduced, it should be made clear which definition is to be understood. Sometimes this can readily be inferred from the context but at other times it may be necessary to state the matter explicitly in order to avoid confusion. At any rate, the beginner should be informed early as regards the significance of these various definitions and that contradictions are likely to arise therefrom.

Another fundamental question which may give rise to contradictory results on the part of the student of group theory has recently presented itself to me in very definite form by the assertion in C. J. Keyser's *Mathematical Philosophy*, 1922, page 204, that when all the positive and negative rational integers, including zero, are combined according to subtraction they do *not* constitute a group. While I am not inclined to call this assertion incorrect I would have been inclined to agree also with Professor Keyser if he had stated that they *do* constitute a group. While these assertions are evidently contradictory, it depends entirely on what is understood by the rule of combination of the elements of a group whether the one or the other is correct. If each of the rational integers is understood to represent the operation of subtracting it from something; that is, if the integer n is understood to mean that n is to be subtracted, then these integers, together with zero, evidently do constitute the same group as when they are combined by addition.

On the other hand, if S_1 and S_2 represent any two of these integers and if when S_1 and S_2 are combined it means that the integer represented by S_2 is to be subtracted from that represented by S_1, or vice versa, it is evident that the associative law is not satisfied since $S_1 - S_2 - S_3$ is not generally equal to $S_1 - (S_2 - S_3)$. It should, however, be noted that when S_1, S_2, S_3 represent ordinary substitutions, and if by the product $S_1 \cdot S_2$ we should mean that the substitution S_2 were to be performed on S_1; that is, if $S_1 \cdot S_2$ should be understood to mean $S_2^{-1}S_1S_2$, then the associative law would also not be satisfied by the ordinary substitutions. By combining two substitutions we do not mean that the second substitution is to be applied on the first but we mean merely that one of these substitutions is to be followed by the other.

It would seem natural to say that the substitutions of a group are combined according to the rule of substitutions. In this case, we would mean thereby that the symbols of our group would represent substitutions and that the rule of combination of these symbols was determined by the properties of these substitutions. In any group in which the elements represent definite operations the law of combination of these elements is determined by the properties of the elements. The principal thing is the properties of the elements. The law of combination of the elements, being deduced from these properties, may be regarded as secondary.

I emphasize these points here because from some of the well-known definitions of an abstract group one might naturally conclude that the law of combination of the elements was of primary importance in group theory and that the properties of the elements themselves played a secondary rôle, while just the opposite seems to me to be the case. In the definition of an abstract group it would seem desirable to state explicitly that the law of combination of the elements is deduced from the properties of the elements. In particular, if we speak of groups whose elements are the rational positive and negative integers together with zero, and if we say that these integers are to be combined according to the rule of subtraction, it would seem to me natural to say that a symbol like 4 was to be construed to mean that the number represented by this symbol was to be subtracted, while the symbol -4 was to be regarded as meaning that the number -4 was to be subtracted, or that 4 was to be added.

If this is done, each of these numbers represents a certain operation which may be applied on something outside of the group. In fact, a group generally looks outside of itself for its main fields of usefulness and the law of combination of its elements is normally construed by this outward look as may be inferred from the fact that this law is commonly denoted by the single operation multiplication. In looking outward it seems to me that we must say that the operations of performing ordinary substitutions, as well as rational integers when combined by subtraction, obey the associative law. In confining our view to the system of elements themselves one may still construe the combination of these elements in such a way that the associative law is satisfied but in this case it may seem more natural to say that the associative law is not satisfied when the elements are combined by subtraction.

The fundamental nature of these remarks may be inferred from the fact that Professor Keyser was writing for the educated laymen and not mainly for the mathematicians. The above remarks therefore show that even those who are not professional mathematicians may come across contradictions in this field if they are so fortunate as to catch the spirit of the group concept, which Professor Keyser pictured for them not only in our commonplace mundane surroundings but also in the movements of the heavenly messengers of good tidings to those who are faithful to the end, as is evidenced by the group of angel flights.

He even raises the question: "Is mind a group?" and states that "it may be that a genius of the so-called universal type—an Aristotle, for example, or a

Leibniz or a Leonardo da Vinci—is one whose mind has the group property." This possible fact may serve to explain some of the extraordinary claims made for group theory which many would be inclined to say could be readily contradicted if they had not been made by men of such eminence. For instance, one of the last public utterances of H. Poincaré was that "the theory of groups is, so to say, entire mathematics, divested of its matter and reduced to a pure form." [1] I presume that those who are most familiar with the varied scientific activities of H. Poincaré would be inclined to call him a genius of the universal type.

At any rate, it is true that while some groups are such omnipresent objects that familiarity has blunted our appreciation of their significance there are others which exhibit themselves only to the most gifted or to those who have made a serious search for them. It is a singular fact that the former did not receive any explicit attention until some of the latter were discovered and their rôle in the theory of algebraic equations became apparent. How different mathematical history would be if Archimedes had emphasized the importance of the group concept in the development of our subject. In particular, the later Greeks would then not have been satisfied with one solution of a quadratic equation but they would have recognized that there is no such thing as an equation in one unknown and of degree $n > 1$, but that the so-called equation in one unknown is really one in n unknowns, n being the degree of the equation. They would have seen that in such an equation one has been led to call different things by the same name x in spite of the fact that one may have desired to do otherwise. Algebra is more resourceful than the inventors thereof.

Group theory as an autonomous subject was initiated by looking below the surface and noting that what is denoted by a single symbol x is really not a single number but a composite of n numbers in disguise. It is the mind not the eye that saw these groups, and ever since then it is the groups which the mind sees which have led to many sweeping remarks relating to the scope of their theory. To those of us whose intellectual insight is less keen some of these remarks may appear to be contradicted by facts just because we see these facts only dimly and fail to recognize some deep connections.

A contradiction of a very well-known elementary theorem on substitution groups is found in the 1900 edition of Pascal's *Repertorium der höheren Mathematik*, volume 1, page 32. It is here stated, as well as in the original Italian edition, that an invariant subgroup of a transitive substitution group does *not* involve all the marks or letters of the group. The following sentence is also evidently inaccurate, since the group in question does not necessarily include all the substitutions but only all the positive substitutions. On the same page it is also incorrectly stated that if all the substitutions of a k times transitive group transform a given group into itself, then this group must be at least $k - 1$ times transitive. It is very well known that the holomorph of the regular abelian group of order 2^n and of type $(1, 1, 1, \cdots)$ is triply transitive. In particular, the holomorph of the non-cyclic regular group of order 4 is the symmetric group of degree

[1] *Acta Mathematica*, vol. 38, 1921, p. 145.

4. It is singular that three such obvious errors should appear on the same page of the standard reference work in question.

On page 203 of Keyser's *Mathematical Philosophy* the term "system having the group property" is defined in practically the same way as the term "group in the most general sense" is defined in volume 2, page 243, of tome 1 of the *Encyclopédie des Sciences Mathématiques*. Hence his statement "that in the older literature of the subject they are called groups, or closed systems" is correct but misleading. On page 576 of volume 1 of the *Encyclopédie* there appears a much more restrictive definition of the term group, and no reference is given from either one of these definitions to the other. These two widely different definitions of this term in such a standard work of reference are a reflection of the fact that the word "group" as a technical mathematical term has been employed by good authorities with widely different meanings. It is only natural that this wide difference in meaning has led to contradictions, but it has not produced chaos in the field of group theory, since one can usually determine from the context what meaning is to be assigned to the term in question.

Perhaps many of us would be inclined to think that such an authoritative work as the *Encyclopédie* should have used its influence to secure uniformity as regards the use of the term "group" with a technical meaning. In so far as uniformity reduces suggestiveness it is an evil, especially in the newer fields of our subject. It is much better to encounter contradictions than sterility. In so far as the use of the same term with widely different meanings suggests analogies and common ground which would otherwise escape the reader's notice it is an advantage. On the other hand, clear thinking demands that the technical terms in use have definite meaning in so far as this meaning relates to the main objects of thought under consideration. A man may work very successfully in the ordinary theory of substitution groups, for instance, without considering all the conditions which an abstract group is supposed to satisfy, or without having grasped the reason why the group of Euclidean geometry does not include the similarity transformations but does include the special homothetic transformations in which the coefficients are plus or minus unity.

The most conspicuous contradictions in the literature of group theory naturally appear in the history of this subject since the wide range of topics with which the mathematical historian is inclined to deal makes it very difficult to avoid misinterpretations. As an instance of this difficulty we may refer to the term *simple group*. This term has been used with at least three different meanings. P. Ruffini used its equivalent (permutazione semplice) in his *Teoria generale delle equazioni*, 1799, page 247, for a cyclic group. H. W. Tanner used the same term for a cyclic prime-power group in volume 20, 1888, of the *Proceedings of the London Mathematical Society*, page 70. This obsolete meaning unfortunately slipped into Dickson's *History of the Theory of Numbers*, volume 1 (1919), page 131. It is somewhat singular that the meaning of this term which is now universally adopted, and was introduced by C. Jordan in 1869, *Mathematische Annalen*, volume 1, page 142, is less in accord with the non-technical meaning

of simple than those noted above, for the modern simple groups are really the most difficult groups.

In a semi-serious manner we may refer here to the fact that one of my colleagues recently directed attention to my questionable use of the term *Lagrange's theorem* for the fundamental theorem that the order of a finite group is divisible by the order of each of its subgroups, since Lagrange did not use this theorem with its general meaning.[1] Such a use was made of it by Galois and one might be inclined to change the name of the theorem to *Galois' theorem* just as the name of *Pell's equation* has been changed by many to *Fermat's equation.* In the present case, there is, however, less substantial reason for making the change since Lagrange actually first used the theorem in a special but important case, while Pell had nothing to do with the equation which bears his name. The term *Lagrange's theorem* for the theorem in question was used already by J. Petersen, *De algebraiske Ligningers Theori,* 1877, and became widely known, especially through the German translation of this popular work under the title *Theorie der Algebraischen Gleichungen,* 1878. While it has been widely used it is not found in some of the standard works of reference, including the large German and French mathematical encyclopedias.

In view of the facts that the term *Lagrange's theorem* has appeared in some of the most frequently consulted group theory literature for such a long time, and that the workers in this field are naturally inclined to express their gratitude to Lagrange for his large share in bringing this theorem to the attention of the public, it seems to the present writer that the use of this term is appropriate. The student of the history of our subject is not likely to be misled thereby since he is constantly reminded of the fact that many mathematical terms have grown in richness of meaning with the development of our subject. Netto called the theorem in question "Lagrange's fundamental theorem of the theory of substitutions" in the opening sentence of an article published in the *Mathematische Annalen,* volume 13 (1878), page 249, and a similar term was used for it in the review of this article in the *Jahrbuch über die Fortschritte der Mathematik.* In Jordan's *Traité des substitutions,* 1870, page 25, there appears a heading entitled "Theorems of Lagrange and of Cauchy." It seems likely that this is the source of the term "Lagrange's theorem".

In closing we shall refer to a few conspicuous historical errors relating to group theory which appear in the *Fortschritte.* We do this not because it is unusually easy to find such errors here but because remarks relating to such a standard work are likely to be more effective than if they related to one less generally used. In an article published in the *Bulletin of the American Mathematical Society,* volume 27 (1921), page 459, we referred to a few mathematical errors relating to group theory and appearing in this work. The present remarks may be regarded as an addition thereto.[2]

[1] R. D. Carmichael, *Bulletin of the American Mathematical Society,* vol. 27, 1921, p. 474.

[2] A considerable number of other errors relating to group theory were listed by the present writer in an article published in this MONTHLY, *1913,* 14-20.

We begin with a review found in the latest available volume at the time this address was prepared—viz., volume 45, relating to the publications of 1914–1915. On page 254 thereof appears a review of an article by G. Heussel (misspelled in the *Fortschritte*) entitled "Ueber Gruppen aus zwei Elementen gleicher Ordnung, b und c, die der Bedingung $b^2 = c^{2m}$ genügen." It is at once evident that the letter m in this title is superfluous for if m is odd it must be prime to the order of c and if it is even this order must be the double of an odd number to which m must again be prime. Hence the article in question is devoted to the well-known groups which are generated by two operators having a common square. Moreover, it does not contain any really new theorem; but neither the author of the article nor the reviewer in the *Fortschritte* indicated that we are here dealing with well-known results expressed in a form which differs only slightly from that in which they appeared earlier. This is the more singular because an article on these groups by the present writer appeared about ten years earlier in the same journal in which Heussel published his article.

The special case when each of the two generating operators which have a common square is of order 2 was fully considered by J. de Perott in the *Bulletin de la Société Mathématique de France*, volume 21, 1893, page 62. This case is so simple that others must have recognized it at an earlier date but the *Encyclopédie des Sciences Mathématiques* fails to give any reference relating thereto. It may be noted, in passing, that the references in this encyclopedia relating to the well-known simple group of order 168, tome 1, volume 1, page 563, are misleading. It would appear from these references that Hermite and Brioschi first directed attention to this group while this honor actually is due to Kronecker and Mathieu. The volume in which Mathieu published his results bears an earlier date (1858) than the volume in which Kronecker's results were published (1859), but Kronecker's paper was presented several months before that by Mathieu, and hence it may be just to say that Kronecker first directed attention to this group, as is done in the *Fortschritte*, volume 21, page 142.

The honor of Kronecker in this connection is beclouded by his remarkable display of ignorance in regard to the then available literature relating to substitution groups since he stated, in substance, that the group of order 168 and degree 7 constitutes the first example of a substitution group of degree n and containing more than one regular cyclic subgroup of this order without being either alternating or symmetric. Among the then known substitution groups satisfying this condition is the triply transitive group of degree 6 and of order 120, studied by Hermite and Cauchy more than a decade earlier. The subgroup of order 60 contained in this group is also an example of such a group. The history of the simple group of order 168 is perhaps especially interesting since this is the simple group of next to the lowest composite order.

Hence it may be of interest to note that Brioschi stated incorrectly that two groups of degree 7 and of order 168 exist, *Annali di Matematica*, volume 2 (1859), page 60. It may also be desirable to add that none of these early workers on the simple group of order 168 seems to have recognized that he was actually dealing

with a simple group. The simplicity of this group seems to have been first established in Jordan's *Traité des substitutions,* as a special case. It is well known that Galois first directed attention to the simplicity of the icosahedral group, which is the simple group of lowest composite order. The history of simple groups of composite order has its origin in the works of Galois but finds its first considerable development in the works of Jordan.

The student who is inclined to accept statements found in standard works of reference without attempting to test them as regards accuracy might be referred to page 160 of volume 34 of the *Fortschritte,* where it is stated that W. Burnside proved that a group which admits an automorphism of order 3 has the property that every pair of conjugate operators contained in it are commutative. This is the opening sentence of the review in question and hence it is the more striking since it is so obviously incorrect. To the thinking reader such obvious misstatements on the part of a reviewer are often refreshing since such a reader will readily see that some condition must have been omitted and in supplying this he may secure a deeper insight into the theorem under consideration.

It is evident that the order of the group of isomorphisms of any group G is equal to the number of different possible ordered sets of k independent generators of G such that the αth operator of each of these sets corresponds to the αth operator of a given one of these sets in some automorphism of G where α is any one of the numbers $1, 2, \cdots, k$. In the special case when G is an abelian prime-power group and its k independent generators are a reduced set, all the operators of the same order in such a set of generators may correspond, and the situation becomes unusually clear. It seems questionable whether such obvious facts should be noted in a review as if they were results found in the article under review, as is done in the *Fortschritte,* volume 40, page 192. What is, however, more to the point is that the term *invariant* is used in this particular article, and the review thereof, with an unusual meaning, and the reading of the review is made more difficult thereby as well as by other obscurities which are not removed in the review.

We venture to refer here to a somewhat amusing incident related to the subject under consideration. The able mathematician I. Schur of Berlin stated correctly on page 189 of volume 40 of the *Fortschritte* that the present writer attributed to him an assertion which he did not make and which, moreover, is false. On page 177 of the following volume of the same journal Schur attributed, in turn, to the present writer an assertion which he also did not make and which, moreover, is also false. It is stated here that the present writer asserted that when the Sylow subgroups of order p^m are transformed according to a triply transitive group then the prime number p must exceed 2. That this assertion is false results directly from the fact that in the alternating group of degree 5 the Sylow subgroups of order 4 are evidently transformed according to a triply transitive group. When a reviewer uses somewhat harsh language about a mistake it is perhaps natural for the one who made this mistake to feel a slight relief when he observes that the reviewer's harsh language applies equally to one of his own mistakes even if this does not remove the stain.

The preceding references to reviews in the *Fortschritte* do not imply that the present writer does not believe in critical mathematical reviews. On the contrary, he heartily believes in public criticism since such criticism is much more apt to be fair than private criticism, and most people form their judgment of the works of others from one or the other of these two sources. It is unfortunate but natural that the reviewers for the *Fortschritte* have exhibited wide differences of judgment as regards such reviews. Many of them were non-critical and practically contented themselves with an exhibition of the main results found in the work under review without even distinguishing between what was known earlier and what was then new. A few others were unduly critical as a result of their own ignorance of the subject under review and their youthful ambition to appear wise. On the whole these reviews are, however, very valuable as many of us know from experience and the *Fortschritte* has always been one of the most important mathematical periodicals for those seeking a broad knowledge of our subject.

It was not without misgivings that I ventured to appear before you on such an occasion as a critic of certain minor parts of the literature to which so much of my energy has been devoted. The normal attitude of mind should be to get all the good we can out of the writings of others and to make allowances for shortcomings, for we all admire generosity and many of us feel the need thereof. On the other hand, as teachers it behooves us also to strive hard to guide those who depend on us so that they may avoid the pitfalls which beset their ways. It is, therefore, necessary for us to become also familiar with this less attractive phase of our subject. Criticisms do not necessarily imply that the author thereof feels that he could have done better than the one that is being criticized but only that he feels that he can add another element which will tend to make the truth stand out more brightly. The preceding remarks are to be construed in this spirit.

THE APRIL MEETING OF THE IOWA SECTION.

The tenth regular meeting of the Iowa section of the Mathematical Association of America was held, in conjunction with the thirty-sixth annual meeting of the Iowa Academy of Science, at Drake University, Des Moines, Iowa, on April 29, 1922. The meeting consisted of one session with Professor C. W. EMMONS presiding. There were twenty-five in attendance, including the following twenty members of the Association:

O. W. Albert, E. W. Chittenden, Julia T. Colpitts, C. W. Emmons, Fay Farnum, C. Gouwens, E. C. Kiefer, G. E. King, R. B. McClenon, F. M. McGaw, J. V. McKelvey, Martha McD. McKelvey, I. F. Neff, E. A. Pattengill, J. F. Reilly, H. L. Rietz, Maria M. Roberts, E. R. Smith, G. W. Snedecor, C. W. Wester.

The following officers were elected for 1922–1923: Chairman, C. W. EMMONS, Simpson College; Vice-chairman, I. F. NEFF, Drake University; Secretary-